Docket No.: 60468.300301

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Moreh et al.**

Application No.: **09/827,697** GAU No.: **2155**

Filed: **04/07/2001** Examiner: **TRAN, Phillip B.**

For: **FEDERATED AUTHENTICATION SERVICE**

#17
4-30-04

Honorable Commissioner for Patents
P.O. Box 1450, Alexandria, VA 22313

Attn.: Board of Patent Appeals and Interferences

APPELLANT'S BRIEF (37 C.F.R. 1.192)

This brief is in furtherance of the Notice of Appeal, filed herewith.

The fees required under § 1.17, and any required petition for extension of time for filing this brief and fees there for, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief is transmitted in triplicate. (37 C.F.R. 1.192(a))

A PETITION FOR ACCELERATED EXAMINATION for this case was granted on 12/10/2003, and we respectfully request that handling of this appeal and all further prosecution of this case by the Office proceed accordingly.

Certificate of Mailing (37 CFR 1.8(a))

I hereby certify that this paper (along with any referred to as being attached or enclosed) is being deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to: Commissioner of Patents, P.O. Box 1450, Alexandria, VA 22313.

04/16/2004
(date)

Pat Bellmann
(Signature of Pat Bellmann)

This brief contains these items under the following headings, and in the order set forth below (37 C.F.R. 1.192(c)):

The final page of this brief bears the practitioner's signature.

I REAL PARTY IN INTEREST (37 C.F.R. 1.192(c)(1))

The real party in interest in this appeal is Secure Data In Motion, Inc., a Delaware corporation of 1875 South Grant Street, 10th Floor, San Mateo, CA 94402, which is assignee of the entire right, title and interest to the invention in the United States and in all foreign countries.

II RELATED APPEALS AND INTERFERENCES (37 C.F.R. 1.192(c)(2))

With respect to other appeals or interferences that will directly affect, or be directly effected by, or have a bearing on the Board's decision in this appeal, there are no such appeals or interferences.

III STATUS OF CLAIMS (37 C.F.R. 1.192(c)(3))

The status of the claims in this application is:

A. TOTAL NUMBER OF CLAIMS IN THE APPLICATION

Claims in the application are: 1-41

(Note, the Advisory Action dated 02/17/2004 wrongly states that claims 1-42 are pending.)

B. STATUS OF ALL OF THE CLAIMS

1. Claims canceled: None
2. Claims withdrawn from consideration but not cancelled: None
3. Claims pending: 1-41 (All)
4. Claims allowed: None
5. Claims rejected: 1-41 (All)

C. CLAIMS ON APPEAL

The claims on appeal are: 1-41

IV STATUS OF AMENDMENTS (37 C.F.R. 1.192(c)(4))

It is Appellant's understanding that all amendments have been entered, as confirmed by the Advisory Action dated 02/17/2004.

V SUMMARY OF INVENTION (37 C.F.R. 1.192(c)(5))

With reference to FIG. 1 of the application it can be seen that Appellants' invention comprises apparatus and methods for authenticating a subject (20), residing in a subject domain (12) on a network, to a server application (38) residing in a server domain (18). For this the subject uses a client (22). The client authenticates the subject to a protocol proxy (34) residing in an authentication domain (16), by providing the protocol proxy with client credentials. [How the client obtains such from an agent domain (14) is shown in the right half of FIG. 1, but is not germane to this appeal.] As needed, the protocol proxy translates data about the client and subject, translates protocols as needed, and communicates the client's request onward to an authentication mechanism (32). Upon successful authentication, the authentication mechanism responds back to the protocol proxy by providing optional attributes and specific access rights for the subject that are appropriate for it to use to access the server application. From these, the protocol proxy creates a name assertion and optional entitlements that it transmits back to the client. The client is now able to access the server application by presenting the name assertion and entitlements, and thus work with the server application thereafter.

Aside from the well-known concept of parties (e.g., the subject/client and the server application) employing trusted third-parties (e.g., the authentication mechanism), a core concept used in this invention is the "name assertion." A name assertion is a type of credential. More specifically, here it is a digitally signed data structure containing a declaration of identity which is presentable to establish a claimed identity. The following are some points and brief definitions related to other concepts that may, optionally, be used in the course of the above.

Many different parties can use name assertions. Thus, the name assertion described above can be termed a "client name assertion," since it asserts the identity of the client. Of course, a client might acquire multiple name assertions, to identify itself to multiple server applications (or to an agent (24) in the agent domain, etc.). The protocol proxy also may use a proxy name

assertion to assert its identity. After all, the client may want to be sure that it can trust in the protocol proxy on the other side of the boundary between the subject and authentication domains.

An "entitlement" is an assertion that a bearer is permitted to have and use something. A name assertion may be accompanied by a digitally signed entitlement. For instance, company ABC's employee J. Doe (a subject with client) may only be allowed to access company XYZ's systems (server application) by presenting ABC's name assertion and a signed entitlement showing that ABC has granted J. Doe the right to use its name assertion.

A S2ML document can be used to contain a name assertion. S2ML is the industry acronym for Security Services Markup Language, a draft standard for communicating security information using extensible markup language (XML).

An adapter is simply a software element. For example, in the present context an adapter can be part of or can be used in front of a server application if it is not able to directly handle name assertions. Adapters can be implemented in any suitable programming language, including XML. The mere fact that an adapter is present or employed is of little significance, whereas the nature of what an adapter is employed to do can be of great significance.

Finally, a few items of terminology merit clarification. The phrase "signed name assertion" is sometimes used in the application. This may seem redundant, since a name assertion is defined as being digitally signed. It may be helpful here to think of how we speak of checks (e.g., a paycheck), regardless of whether one has been signed or not. Thus, a signed name assertion is one that is complete, and ready for use. It was noted that the first name assertion discussed above could be termed a "client name assertion." In the claims, however, the phrase "authentication name assertion" is used. This was done to emphasize in the independent claims that the name assertion there is used to authenticate the client to the server application, and thus to hopefully avoid this key element being superficially misinterpreted.

VI ISSUES (37 C.F.R. 1.192(c)(6))

A. Whether claims 1-15 and 22-35 are anticipated by BARU et al., "The SDSC Storage Resource Broker," ACM, 1998 (hereinafter, Baru), and thereby unpatentable under 35 U.S.C. § 102(b).

B. Whether claims 16 and 36 are obvious over Baru in view of "admitted prior art" (hereinafter, APA), and thereby unpatentable under 35 U.S.C. § 103(a).

C. Whether claims 17-21 and 37-41 are obvious over Baru in view of Hele et al., U.S. Pat. App. Pub. No. US 2002/0120474 (hereinafter, Hele), and thereby unpatentable under 35 U.S.C. § 103(a).

VII GROUPING OF CLAIMS (37 C.F.R. 1.192(c)(7))

The grouping of the claims for purposes of this appeal is:

A. Claims 1-15 and 22-35.

B. Claims 16 and 36.

C. Claims 17-21 and 37-41.

VIII ARGUMENTS (37 C.F.R. 1.192(c)(8))

A. CLAIMS 1-15 AND 22-35 ARE NOT ANTICIPATED BY BARU

(35 U.S.C. § 102(b))

> "*A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference.*" Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). And, "*the elements must be arranged as required by the claim ....*" MPEP 2131 discussing In re Bond, 910 F.2d 831, 15 USPQ2d 1566 (Fed. Cir. 1990).

We respectfully submit that a *prima facie* case for anticipation has not been established here because numerous elements of the claimed invention are not described in Baru. In the alternative, should it be found that a *prima facie* case has been established, we urge that it is rebutted by the following.

It may be helpful to compare Baru's Figure 2 (page 5) with Fig. 1 of the application when reading the following, so copies are here provided:

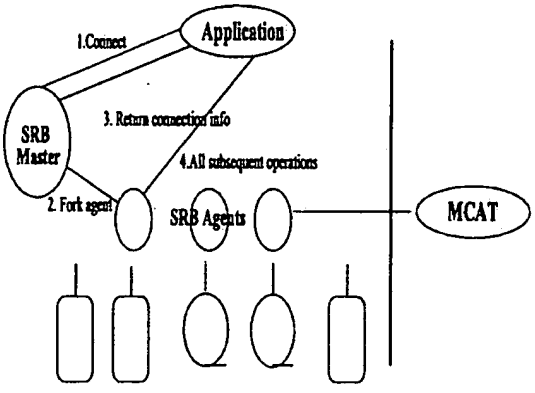


Figure 2: The SRB Process Model.

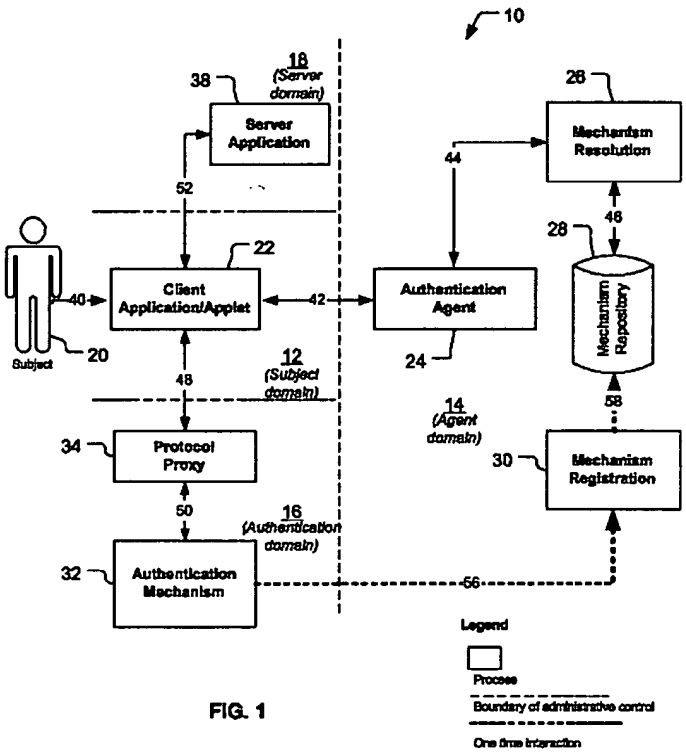


FIG. 1

Since the Advisory Action, paper no. 15, dated 02/17/2004, adds no new argument, we herein cite to the Office Action with final rejections (hereinafter "Action"), paper no. 13, dated 02/03/2004.

The Action wrongly states:

> *Regarding claim 1, Baru teaches a system ... comprising:*
> *a client for ... authenticating the subject to other components of the system by providing client credentials on behalf of the subject, ... [see Fig. 2 and Sec. 3 on Page 5]; and*
> *a protocol proxy for communicating between said client and the authentication mechanism and for authenticating said client based on said client credentials, for obtaining from the authentication mechanism temporary credentials for said client to access the server application, and for creating from said temporary credentials an authentication name assertion allowing said client to access the server application [see Secs. 2.8-2.10 on Page 4 and Sec. 3 on Page 5].*

The Examiner has apparently taken Baru's client/application ("Application in its figures and "client" in its text) as equivalent to Appellant's client (22), since Baru's client/application connects and authenticates to its SRB master. We do not agree, for reasons that become clear below.

[Regrettably, the record is quite unclear just what elements and steps in the respective inventions the Examiner thinks are analogous, since all three actions essentially parrot the language of claim 1, assert that Baru teaches it, and otherwise say very little else that is helpful in this respect. We have asked for clarification in our Responses to the Office Actions – and those requests have been ignored.]

The Examiner has perhaps taken Baru's SRB master as equivalent to our protocol proxy (34), but the error in this is that Baru's SRB master performs all authentication and Appellant's protocol proxy (34) does not do this. It instead receives our client credentials, and then based on them works with an authentication mechanism (32) to obtain temporary credentials it uses to create an authentication name assertion for Appellant's client (22) to use to gain access to a server application (38). It follows that Baru's SRB master cannot be equivalent to Appellant's protocol proxy (34).

[Although not argued in prosecution, it might seem that SRB master could be equated to the combination of both of Appellant's protocol proxy (34) and authentication mechanism (32). However, this is rebuttable in many ways. For example, the following discussion shows that the directions of communication between the various elements in the respective inventions are

different. Also, Baru teaches just one SRB master because its scheme has need for only one. In contrast, one of Appellant's clients (22) often will work with multiple protocol proxies (34).]

Perhaps the Examiner has instead taken Baru's SRB agent as equivalent to Appellant's protocol proxy (34). If so, this is also wrong. Baru's client/application first communicates ("*1. Connect*" in its Figure 2) with its SRB master, and then its SRB master communicates ("*2. Fork agent*") with one of its many SRB agents, and then its SRB master communicates back ("*3. Return connection info*") to its client/application; and then its client/application communicates ("*4. All subsequent operations*") with the SRB agent that was delegated. This triangular set of communications in Baru, with its SRB agent at one vertex, cannot be reconciled with Appellant's protocol proxy (34), since the path in claim 1 is linear, i.e., Client – Protocol Proxy – Authentication Mechanism – Protocol Proxy – Client.

Furthermore, Baru's SRB agent cannot be equated to Appellant's protocol proxy because the ordering of communications is different. In claim 1, the protocol proxy communicates to the authentication mechanism to obtain temporary credentials, to use to create the authentication name assertion that allows the client to itself access the server application. Baru's SRB agent does not use this order of communications, it only acts after delegated to do so by the SRB Master. Also, in claim 1 the protocol proxy communicates between the client and the authentication mechanism. Baru's SRB agent also does not use such a route.

Still further, Baru's SRB agent cannot be equivalent to Appellant's protocol proxy because the intermediaries used are different. Appellant's authentication name assertion allows the client to itself – thereafter – carry on with the server application. In Baru, "*The client uses the SRB Agent for all subsequent communications*" (pg. 5, left col., step 4), thus remaining a permanent intermediary between its client/application and the resources it needs.

Yet further, in Baru the SRB master "*forks a SRB Agent to service the authenticated connection and returns the connection handle to the client.*" Whereas, in claim 1 the protocol proxy provides Appellant's client with an authentication name assertion that allows it to access the server application. As those of ordinary skill in the art well know, a "connection handle" and an "authentication name assertion" are not analogous. These are terms of art having quite different meanings (as is "credential, " from which the "authentication name assertion" here is created).

While most of the discussion above has been about the protocol proxy, it should also be clear now that Baru does not teach or reasonably suggest any of the client, protocol proxy, authentication mechanism, or server application of Appellant's claim 1. Claims 2-15 depend from claim 1, so it follows that Baru also does not teach or reasonably suggest elements of these claims. Similarly, claims 22-35 recite a method having steps that work with a client, protocol proxy, authentication mechanism, and server application as in claim 1, so it also follows that Baru also does not teach or reasonably suggest the steps of these claims.

In sum, a *prima facie* case for anticipation of claims 1-15 and 22-35 has not been made or is now completely rebutted, and these claims should now be allowed.

B. CLAIMS 16 AND 36 ARE NOT OBVIOUS OVER BARU IN VIEW OF APA (35 U.S.C. § 103(a))

> *To establish a prima facie case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on applicant's disclosure.* MPEP §2142

A *prima facie* case for obviousness has not been established here because the rejection fails to meet the first and third criteria. In the alternative, should it somehow be found that a *prima facie* case has been established, we urge that it is rebutted by the following.

1. There is no suggestion or motivation to combine Baru and APA

The APA here is the well-known Secure Remote Password (SRP) protocol, which the Action notes is useful "*for authenticating clients to the remote servers in a secure fashion.*" With reference again to Figure 2 of Baru and FIG. 1 of the present application, the whole point of the respective inventions is to permit Baru's clients/applications and Appellant's clients to get at secured resources. Granted, Baru's client/application might possibly use SRP to authenticate to the SRB master, but that is only one third of the way to the secured resource. Baru's client/application could not use SRP to authenticate to the SRB agent, the next step of the way to the secured resource, since that would eliminate Baru's need for steps 2-3 (pg. 5, left col.) where

"*The SRB Master forks* [the] *SRB Agent to service the authenticated connection and returns the connection handle to the client" (emphasis added).* By using SRP ("*where the server carries a verifier that allows it to authenticate the client*" ADA, Appellant's application at pg. 2, ln. 2), there would be no need for the SRB master to fork the SRB agent. Also, in Baru the whole gist of the invention is that the client/application authenticates to the SRB agent using the connection handle. A connection handle and a verifier are not analogous, and substituting a SRP verifier for the connection handle of Baru would change Baru's entire principle of operation. This means that there cannot be a proper suggestion or motivation to combine Baru and APA, since MPEP 2143.01 provides the guidance:

> *"If the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims prima facie obvious."* In re Ratti, 270 F.2d 810, 123 USPQ 349 (CCPA 1959)

2. The combination of Baru and APA does not teach or reasonably suggest all of the claim limitations

Since Baru does not contribute what it has been relied upon to contribute, and since ADA (the mere fact that SRP exists and is well-known) also does not remedy the deficiencies of Baru, it follows that the combination of Baru and ADA cannot teach or reasonably suggest the claimed invention.

3. Claims 16 and 36 should now be allowed

We have shown above that the rejection of claim 16 is unfounded. Claim 36 recites a method having steps that work with the same elements as in claim 16, so it follows that the combination of Baru and ADA also cannot teach or reasonably suggest the steps of claim 36.

In sum, a *prima facie* case for obviousness of claims 16 and 36 has not been established or is now completely rebutted, and these claims should now be allowed.

C. CLAIMS 17-21 AND 37-41 ARE NOT OBVIOUS OVER BARU IN VIEW OF HELE (35 U.S.C. § 103(a))

The criteria to establish a *prima facie* case for obviousness are stated above. Such a case has not been established here because the rejection fails to establish the first and third criteria. In the alternative, should it be found that a *prima facie* case has been established, we urge that it is rebutted by the following.

1. There is no suggestion or motivation to combine Baru and Hele

The Action cites only paragraph [0054] of Hele, which states:

> *The carrier policy support server 102 produces electronic documents to authenticate the policy, e.g., documents requiring a user's signature or a user's electronic signature, and can issue these through the business-to-business transaction server 100 to the appropriate insurance carrier 104. The communication between the business-to-business server 100 and the insurance carrier 104 can be made secure using the adaptor security layer 110 and various internet and network protocols, e.g., protocols accepted by an XML/HTTP(s) adapter 112, an HTML/HTTP(s) adaptor 114, an FTP adaptor 116, an SMTP/IMAP adaptor 118, and a proprietary adaptor 120.* (emphasis added)

The use of an "*adaptor security layer*" is a completely different approach than Appellant's use of client credentials, an authentication mechanism, temporary credentials, and an authentication name assertion. This means that there cannot be a proper suggestion or motivation to combine Baru and APA (see e.g., MPEP 2143.01 citing In re Ratti, quoted above).

2. The combination of Baru and Hele does not teach or reasonably suggest all of the claim limitations

The Action states:

> *Regarding* [claims 17-21 (previously mislabeled "18-22")], *Baru does not explicitly teach* [that the] *protocol proxy produces a signed name assertion wherein said signed name assertion is contained in a S2ML document and wherein said protocol proxy further produces a signed name entitlement and wherein said protocol proxy uses a proxy name assertion to authenticate itself to the client and there is an adapter for receiving said authentication name assertion, recreating said credentials, and permitting said client to access the server application based on said credentials. However, the use of XML adapter for authentication purpose is well-known in the art as disclosed by Hele [Paragraph 0054].* (emphasis added)

However, aside from the statements about what Baru does not teach, none of this is correct.

It is helpful here to focus on the claims and the actual elements in them. Claim 17 recites that the "*protocol proxy produces a signed name assertion,*" but "*A name assertion is a type of credential. More specifically ... a digitally signed data structure containing a declaration of identity which is presentable to establish a claimed identity.*" (Appellant's application pg. 7, ln. 25-27). Claim 18 recites that the "*signed name assertion is contained in a S2ML document,*" but S2ML is merely the industry acronym for Security Services Markup Language, a draft XML standard for communicating security information (see e.g., Appellant's application pg. 19, ln. 4-5). Claim 19 recites that the "*protocol proxy further produces a signed name entitlement,*" but an entitlement is simply what it implies, a proof that the bearer of something is permitted to have and properly has it. An example appears in Appellant's application (pg. 15, ln. 2, et seq.) of an employer using entitlements for its employees to use the employer's name assertion. Thus, in the present context and to one of ordinary skill in the art, a "signed name entitlement" is a digitally signed entitlement proving the right to use a name assertion. Claim 20 recites that the "*protocol proxy uses a proxy name assertion to authenticate itself to the client,*" and this should have clear meaning in view of the above. And claim 21 (depending from claim 1) recites "*further comprising an adapter for receiving said authentication name assertion, recreating said credentials, and permitting said client to access the server application based on said credentials,*" and the elements of this should also be clear. An adapter is, of course, simply important in the context of what it does.

The point of all of this is that Hele does not teach or reasonably suggest the use of any of name assertions, used by a client or protocol proxy, or signed or otherwise; S2ML, much less S2ML documents containing a signed name assertion; name entitlements, signed or otherwise; or an adapter for receiving such to provide credentials for a client to access a server application. Notably, the Action nowhere cites any support otherwise.

Paragraph [0054] of Hele (quoted in its entirety above) merely states "... *communication ... can be made secure using the adaptor security layer 110 and various internet and network protocols, e.g., protocols accepted by an XML/HTTP(s) adapter 112 ....*" However, this merely teaches the use of extensible markup language (XML), and that communications "*can be made secure using* [an] *adaptor security layer 110 and ... protocols accepted by an XML/HTTP(s) adapter ....*" Hele nowhere reasonably suggests S2ML. In fact, it teaches away from using it,

instead teaching its "*adaptor security layer 110*". The XML adapter of Hele is merely a software interface able to handle communications in some protocols, with disregard for the content of those communications (by they for authentication purposes or otherwise).

As previously shown, Baru does not contribute what it has been relied upon to contribute to support the rejection. Hele does not, and has never been asserted to, remedy the deficiencies of Baru. Also, as just shown, Hele does not teach or reasonably suggest any of what the Action relies upon it to contribute to support the rejection. Accordingly, the combination of Baru and Hele cannot teach or reasonably suggest the subject matter of claims 17-21.

3. Claims 17-21 and 37-41 should now be allowed

We have shown above that the rejection of claims 17-21 is unfounded. Claims 37-41 recite a method having steps that work with the same elements as in claims 17-21, so it follows that the combination of Baru and Hele also cannot teach or reasonably suggest the steps of claims 37-41.

In sum, a *prima facie* case for obviousness of claims 17-21 and 37-41 has not been established or is now completely rebutted, and these claims should now be allowed.

D. COMMENTS ON OTHER ARGUMENT IN THE ACTION

The Action includes an extensive Response to Arguments section, to which Appellant remarked in detail in its Response dated 02/10/2004. Since the Examiner's comments in the Response to Arguments are not formally part of the statements of rejection, we do not address them here. However, should any of those comments somehow be felt to be probative Appellant respectfully asks that its remarks in its Response then also be considered.

E. SUMMARY

As has been shown herein, the Examiner has erred by finding anticipation and obviousness where such are not supported by the art cited. We respectfully ask the Board to reverse the Examiner and to now permit passage to issue of claims 1-41 (Groups A-C, consisting of all of the claims in the case).

IX APPENDIX OF CLAIMS INVOLVED IN THE APPEAL (37 C.F.R. 1.192(c)(9))

1. A system for authenticating a subject residing in a subject domain on a network to a server application residing in a server domain on the network, wherein an authentication mechanism residing in an authentication domain on the network affects the service provided by the server application, the system comprising:

a client for communicating with other components of the system and for authenticating the subject to other components of the system by providing client credentials on behalf of the subject, wherein said client also resides in the subject domain; and

a protocol proxy for communicating between said client and the authentication mechanism and for authenticating said client based on said client credentials, for obtaining from the authentication mechanism temporary credentials for said client to access the server application, and for creating from said temporary credentials an authentication name assertion allowing said client to access the server application.

2. The system of claim 1, wherein:

the subject is non-human and said client is integrated into the subject; and

said client gathers subject credentials for the subject and communicates said subject credentials to said protocol proxy.

3. The system of claim 1, wherein a plurality of the authentication mechanisms are present on the network, and the system further comprising:

an agent for communicating with other components of the system and for interacting with said client to chose an appropriate authentication mechanism from among said plurality of the authentication mechanisms, wherein said agent resides in an agent domain on the network.

4. The system of claim 3, wherein said client interacts with said protocol proxy to determine a specification of the authentication mechanism and said client communicates said specification to said agent.

5. The system of claim 3, wherein said client includes a callback mechanism for determining said appropriate authentication mechanism for the server application from among said plurality of the authentication mechanisms.

6. The system of claim 5, wherein said callback mechanism interacts with the subject to determine said appropriate authentication mechanism.

7. The system of claim 5, wherein said callback mechanism accesses a configuration repository to determine said appropriate authentication mechanism.

8. The system of claim 3, wherein said agent includes a mechanism resolver for determining from said plurality of the authentication mechanisms a subset of zero or more of the authentication mechanisms which affects the service provided by the server application.

9. The system of claim 8, wherein said agent further includes an authentication agent for brokering between said client and said mechanism resolver.

10. The system of claim 8, wherein said agent further includes a mechanism repository for storing information about said plurality of the authentication mechanisms and said mechanism resolver queries said mechanism repository when determining said subset of zero or more of the authentication mechanisms which affects the service provided by the server application.

11. The system of claim 10, wherein said agent further includes a mechanism registrator for the authentication mechanism to register in said mechanism repository by adding information about itself.

12. The system of claim 11, wherein said mechanism registrator is further for the authentication mechanism to update itself in said mechanism repository by changing information about itself.

13. The system of claim 4, wherein said protocol proxy resides in said agent domain on the network.

14. The system of claim 1, wherein said protocol proxy resides in the authentication domain on the network.

15. The system of claim 1, wherein said protocol proxy uses a standard security protocol to communicate with said client and a mechanism-specific protocol to communicate with the authentication mechanism.

16. The system of claim 1, wherein at least one of said client and said protocol proxy authenticates using SRP protocol.

17. The system of claim 1, wherein said protocol proxy produces a signed name assertion.

18. The system of claim 17, wherein said signed name assertion is contained in a S2ML document.

19. The system of claim 17, wherein said protocol proxy further produces a signed name entitlement.

20. The system of claim 1, wherein said protocol proxy uses a proxy name assertion to authenticate itself to the client.

21. The system of claim 1, further comprising an adapter for receiving said authentication name assertion, recreating said credentials, and permitting said client to access the server application based on said credentials.

22. A method for authenticating a subject residing in a subject domain on a network to a server application residing in a server domain on the network, wherein an authentication mechanism

residing in an authentication domain on the network affects the service provided by the server application, the method comprising the steps:

(a) authenticating the subject to a protocol proxy with a client by providing subject credentials on behalf of the subject;

(b) obtaining a name assertion from said protocol proxy via the authentication mechanism which will allow said client to access the server application, thereby mediating between said protocol proxy and the authentication mechanism to permit the subject to access the server application via said client;

(c) creating an authentication name assertion with said protocol proxy based on said subject credentials which will allow said client to access the server application;

(d) communicating said authentication name assertion to said client; and

(e) communicating said authentication name assertion to the server application.

23. The method of claim 22, wherein the subject is non-human and said client is integrated into the subject, and the method further comprising:

gathering said subject credentials with said client for the subject; and

communicating said subject credentials to said protocol proxy.

24. The method of claim 23, wherein a plurality of the authentication mechanisms are present on the network, and the method further comprising:

interacting between said client and an agent to chose an appropriate authentication mechanism from among said plurality of the authentication mechanisms, wherein said agent resides in an agent domain on the network.

25. The method of claim 24, further comprising:

interacting between said client and said protocol proxy to determine a specification of the authentication mechanism; and

communicating said specification with said client to said agent.

26. The method of claim 24, further comprising determining an appropriate authentication mechanism for accessing the server application from among said plurality of the authentication mechanisms.

27. The method of claim 26, further comprising interacting with the subject to determine said appropriate authentication mechanism.

28. The method of claim 26, further comprising accessing a configuration repository to determine said appropriate authentication mechanism.

29. The method of claim 26, further comprising:

(f) resolving from said plurality of the authentication mechanisms a subset of zero or more of the authentication mechanisms which affects the service provided by the server application.

30. The method of claim 29, wherein said agent further includes an authentication agent, and the method further comprising:

brokering between and authentication agent and said client in said step (f).

31. The method of claim 29, wherein said agent domain further includes a mechanism repository, and the method further comprising:

storing information about said plurality of the authentication mechanisms in said mechanism repository; and

querying said mechanism repository in said step (f).

32. The method of claim 31, further comprising registering the authentication mechanism in said mechanism repository by adding information about the authentication mechanism.

33. The method of claim 24, wherein said protocol proxy resides in said agent domain on the network.

34. The method of claim 22, wherein said protocol proxy resides in the authentication domain on the network.

35. The method of claim 22, wherein said protocol proxy uses a standard security protocol to communicate with said client and a mechanism-specific protocol to communicate with the authentication mechanism.

36. The method of claim 22, wherein at least one of said client and said protocol proxy authenticates using SRP protocol.

37. The method of claim 22, wherein said protocol proxy produces a signed name assertion.

38. The method of claim 37, wherein said signed name assertion is contained in a S2ML document.

39. The method of claim 37, wherein said protocol proxy further produces a signed name entitlement.

40. The method of claim 22, wherein said protocol proxy uses a proxy name assertion to authenticate itself to the client.

41. The method of claim 22, further comprising an adapter, and the method further comprising:

receiving said authentication name assertion with said adapter;

recreating said credentials with said adapter; and

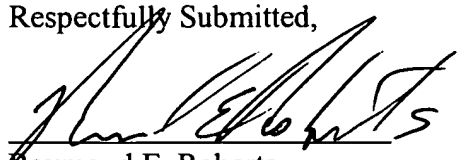
permitting said client to access the server application based on said credentials.

*

Intellectual Property Law Offices
1901 S. Bascom Ave., Suite 660
Campbell, CA 95008

Telephone: 408.558.9950
Facsimile: 408.558.9960
E-mail: RRoberts@iplo.com

Respectfully Submitted,



Raymond E. Roberts
Reg. No.: 38,597